This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

        1-105   (Cancelled)

        106.   (Currently Amended) In combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and encryption functions, a method of obtaining the black box by the DRM system from a black box server, the method comprising:

        requesting, by the DRM system, [[the]] a first black box from the black box server;

        generating, by the black box server, the first black box, such generated first black box being unique and having a public / private key pair and ~~functionality necessary to employ such~~ electronic code for employing the key pair within the DRM system on the computing device;

        delivering, by the black box server, the generated first black box to the DRM system; and

        installing, by the DRM system, the delivered first black box in such DRM system,

        the DRM system further providing code for periodically determining whether the first black box is current or not current and for upgrading at least the public / private key pair in the first black box from the black box server to result in a second black box when the first black box is not current.

107.   (Withdrawn) The method of claim 106 wherein the DRM system has

a previously installed black box prior to the requesting step, the method further comprising

determining prior to the requesting step that the previously installed black box is non-unique.

108.   (Withdrawn) The method of claim 106 wherein the DRM system has

a previously installed black box prior to the requesting step, the method further comprising

determining prior to the requesting step that the previously installed black box is not current.

109.   (Original)   The method of claim 106 wherein the requesting step

comprises requesting the black box by way of a network connection to the black box server.

110.   (Original)   The method of claim 109 wherein the requesting step

comprises requesting the black box by way of an Internet connection to the black box server.

111.   (Withdrawn) The method of claim 106 wherein the DRM system has

a first previously installed black box prior to the requesting step, the first previously installed

black box having a public / private key pair different from the public / private key pair of the

generated black box, and wherein the generating step includes providing the generated black

box with the public / private key pair of the first previously installed black box.

112.   (Withdrawn) The method of claim 111 wherein the DRM system had

a second previously installed black box prior to having the first previously installed black

box, the second previously installed black box having a public / private key pair different

Page 3 of 23

from the public / private key pair of the first previously installed black box and also different

from the public / private key pair of the generated black box, and wherein the generating step

further includes providing the generated black box with the public / private key pair of the

second previously installed black box.

113.   (Withdrawn)   The method of claim 106 wherein the generating step

includes providing the generated black box with an identifier indicative of currency.

114.   (Withdrawn)   The method of claim 113 wherein the generating step

includes providing the generated black box with a version number.

115.   (Withdrawn)   The method of claim 106 wherein the generating step

includes providing the generated black box with a digital certificate.

116.   (Withdrawn)   The method of claim 115 wherein the generating step

includes providing the generated black box with a digital certificate proffering that the

generated black box should be trusted.

117.   (Withdrawn)   The method of claim 106 wherein the generating step

includes encrypting at least a portion of the private key of the generated black box according

to a code-based encryption technique.

from the public / private key pair of the first previously installed black box and also different

from the public / private key pair of the generated black box, and wherein the generating step

further includes providing the generated black box with the public / private key pair of the

second previously installed black box.

113.   (Withdrawn)   The method of claim 106 wherein the generating step

includes providing the generated black box with an identifier indicative of currency.

114.   (Withdrawn)   The method of claim 113 wherein the generating step

includes providing the generated black box with a version number.

115.   (Withdrawn)   The method of claim 106 wherein the generating step

includes providing the generated black box with a digital certificate.

116.   (Withdrawn)   The method of claim 115 wherein the generating step

includes providing the generated black box with a digital certificate proffering that the

generated black box should be trusted.

117.   (Withdrawn)   The method of claim 106 wherein the generating step

includes encrypting at least a portion of the private key of the generated black box according

to a code-based encryption technique.

118.   (Withdrawn) The method of claim 117 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to software code associated with the generated black box, whereby adulteration of such software code prevents such private key from being decrypted.

119.   (Original)   The method of claim 106 wherein the generating step includes associating the generated black box with the DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device.

120.   (Original)   The method of claim 119 wherein the requesting step includes providing information unique to the DRM system / computing device, and wherein the generating step includes generating the black box based in part on the provided information, whereby the generated black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

121.   (Original)   The method of claim 119 wherein the DRM system / computing device is a first DRM system / computing device, wherein the generating step includes associating the generated black box with the first DRM system / computing device and also with a second DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

Page 5 of 23

PATENT

122.   (Currently Amended) In combination with a digital rights management

(DRM) system operating on a computing device, the DRM system requiring a black box for

performing decryption and encryption functions, a method of obtaining the black box by the

DRM system, the method comprising:

requesting [[the]] a first black box from a black box server, the black box

server thereafter generating the first black box, such first generated black box being unique

and having a public / private key pair and functionality necessary to employ such electronic

code for employing the key pair within the DRM system on the computing device;

receiving the generated first black box from the black box server; and

installing the received first black box in such DRM system,

the DRM system further providing code for periodically determining whether

the first black box is current or not current and for upgrading at least the public / private key

pair in the first black box from the black box server to result in a second black box when the

first black box is not current.

123.   (Withdrawn) The method of claim 122 wherein the DRM system has

a previously installed black box prior to the requesting step, the method further comprising

determining prior to the requesting step that the previously installed black box is non-unique.

124.   (Withdrawn) The method of claim 122 wherein the DRM system has

a previously installed black box prior to the requesting step, the method further comprising

determining prior to the requesting step that the previously installed black box is not current.

125.   (Original)   The method of claim 122 wherein the requesting step comprises requesting the black box by way of a network connection to the black box server.

126.   (Withdrawn)   The method of claim 125 wherein the requesting step comprises requesting the black box by way of an Internet connection to the black box server.

127.   (Withdrawn)   The method of claim 122 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the requesting step includes providing the public / private key pair of the first previously installed black box to the black box server, whereby the generated black box is provided with the public / private key pair of the first previously installed black box.

128.   (Withdrawn)   The method of claim 127 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the requesting step further includes providing the public / private key pair of the second previously installed black box to the black box server, whereby the generated black box is also provided with the public / private key pair of the second previously installed black box.

125.   (Original)   The method of claim 122 wherein the requesting step comprises requesting the black box by way of a network connection to the black box server.

126.   (Withdrawn)   The method of claim 125 wherein the requesting step comprises requesting the black box by way of an Internet connection to the black box server.

127.   (Withdrawn)   The method of claim 122 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the requesting step includes providing the public / private key pair of the first previously installed black box to the black box server, whereby the generated black box is provided with the public / private key pair of the first previously installed black box.

128.   (Withdrawn)   The method of claim 127 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the requesting step further includes providing the public / private key pair of the second previously installed black box to the black box server, whereby the generated black box is also provided with the public / private key pair of the second previously installed black box.

Page 7 of 23

PATENT

129.   (Withdrawn)   The method of claim 122 wherein the received black box includes an identifier indicative of currency.

130.   (Withdrawn)   The method of claim 129 wherein the received black box includes a version number.

131.   (Withdrawn)   The method of claim 122 wherein the received black box includes a digital certificate.

132.   (Withdrawn)   The method of claim 131 wherein the received black box includes a digital certificate proffering that such received black box should be trusted.

133.   (Withdrawn)   The method of claim 122 wherein at least a portion of the private key of the received black box is encrypted according to a code-based encryption technique.

134.   (Withdrawn)   The method of claim 133 at least a portion of the private key of the received black box is encrypted according to software code associated with such received black box, whereby adulteration of such software code prevents such private key from being decrypted.

129.   (Withdrawn)   The method of claim 122 wherein the received black

box includes an identifier indicative of currency.

130.   (Withdrawn)   The method of claim 129 wherein the received black

box includes a version number.

131.   (Withdrawn)   The method of claim 122 wherein the received black

box includes a digital certificate.

132.   (Withdrawn)   The method of claim 131 wherein the received black

box includes a digital certificate proffering that such received black box should be trusted.

133.   (Withdrawn)   The method of claim 122 wherein at least a portion of

the private key of the received black box is encrypted according to a code-based encryption

technique.

134.   (Withdrawn)   The method of claim 133 at least a portion of the private

key of the received black box is encrypted according to software code associated with such

received black box, whereby adulteration of such software code prevents such private key

from being decrypted.

135. (Original) The method of claim 122 wherein the received black box is associated with the DRM system / computing device, whereby such received black box is inoperable on another DRM system / computing device.

136. (Original) The method of claim 135 wherein the requesting step includes providing information unique to the DRM system / computing device, and wherein the received black box was generated based in part on the provided information, whereby the received black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

137. (Original) The method of claim 135 wherein the DRM system / computing device is a first DRM system / computing device, wherein the received black box is associated with the first DRM system / computing device and also with a second DRM system / computing device, whereby the received black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

138. (Currently Amended) In combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and encryption functions, a method of providing the black box by a black box server, the method comprising:

receiving a request for [[the]] a first black box from the DRM system;

generating the first black box, such generated first black box being unique and

having a public / private key pair and functionality necessary to employ such electronic code

for employing the key pair within the DRM system on the computing device; and

delivering the generated first black box to the DRM system, the delivered first

black box being installed by the DRM system in such DRM system,

the DRM system further providing code for periodically determining whether

the first black box is current or not current and for upgrading at least the public / private key

pair in the first black box from the black box server to result in a second black box when the

first black box is not current.

139. (Original)   The method of claim 138 wherein the receiving step

comprises receiving the request by way of a network connection between the black box

server and the DRM system.

140. (Original)   The method of claim 139 wherein the receiving step

comprises receiving the request by way of an Internet connection between the black box

server and the DRM system.

141. (Withdrawn) The method of claim 138 wherein the DRM system has

a first previously installed black box prior to the requesting step, the first previously installed

black box having a public / private key pair different from the public / private key pair of the

generated black box, and wherein the generating step includes providing the generated black

box with the public / private key pair of the first previously installed black box.

Page 10 of 23

generating the <u>first</u> black box, such generated <u>first</u> black box being unique and

having a public / private key pair and ~~functionality necessary to employ such~~ <u>electronic code</u>

<u>for employing the</u> key pair within the DRM system on the computing device; and

delivering the generated <u>first</u> black box to the DRM system, the delivered <u>first</u>

black box being installed by the DRM system in such DRM system<u>,</u>

<u>the DRM system further providing code for periodically determining whether</u>

<u>the first black box is current or not current and for upgrading at least the public / private key</u>

<u>pair in the first black box from the black box server to result in a second black box when the</u>

<u>first black box is not current.</u>

139.   (Original)   The method of claim 138 wherein the receiving step

comprises receiving the request by way of a network connection between the black box

server and the DRM system.

140.   (Original)   The method of claim 139 wherein the receiving step

comprises receiving the request by way of an Internet connection between the black box

server and the DRM system.

141.   (Withdrawn)   The method of claim 138 wherein the DRM system has

a first previously installed black box prior to the requesting step, the first previously installed

black box having a public / private key pair different from the public / private key pair of the

generated black box, and wherein the generating step includes providing the generated black

box with the public / private key pair of the first previously installed black box.

Page 10 of 23

142.   (Withdrawn) The method of claim 141 wherein the DRM system had

a second previously installed black box prior to having the first previously installed black

box, the second previously installed black box having a public / private key pair different

from the public / private key pair of the first previously installed black box and also different

from the public / private key pair of the generated black box, and wherein the generating step

further includes providing the generated black box with the public / private key pair of the

second previously installed black box.

143.   (Withdrawn) The method of claim 138 wherein the generating step

includes providing the generated black box with an identifier indicative of currency.

144.   (Withdrawn) The method of claim 143 wherein the generating step

includes providing the generated black box with a version number.

145.   (Withdrawn) The method of claim 138 wherein the generating step

includes providing the generated black box with a digital certificate.

146.   (Withdrawn) The method of claim 145 wherein the generating step

includes providing the generated black box with a digital certificate proffering that the

generated black box should be trusted.

147.   (Withdrawn)   The method of claim 138 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to a code-based encryption technique.

148.   (Withdrawn)   The method of claim 147 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to software code associated with the generated black box, whereby adulteration of such software code prevents such private key from being decrypted.

149.   (Original)   The method of claim 138 wherein the generating step includes associating the generated black box with the DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device.

150.   (Original)   The method of claim 149 wherein the receiving step includes receiving information unique to the DRM system / computing device, and wherein the generating step includes generating the black box based in part on the received information, whereby the generated black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

151.   (Original)   The method of claim 149 wherein the DRM system / computing device is a first DRM system / computing device, wherein the generating step includes associating the generated black box with the first DRM system / computing device and also with a second DRM system / computing device, whereby the generated black box is

inoperable on another DRM system / computing device which is not the first or second DRM

system / computing device.

152.   (Currently Amended) A computer-readable medium having computer-

executable instructions thereon for performing a method in combination with a digital rights

management (DRM) system operating on a computing device, the DRM system requiring a

black box for performing decryption and encryption functions, the method for obtaining the

black box by the DRM system and comprising:

requesting [[the]] a first black box from a black box server, the black box

server thereafter generating the first black box, such first generated black box being unique

and having a public / private key pair and functionality necessary to employ such electronic

code for employing the key pair within the DRM system on the computing device;

receiving the generated first black box from the black box server; and

installing the received first black box in such DRM system,

the DRM system further providing code for periodically determining whether

the first black box is current or not current and for upgrading at least the public / private key

pair in the first black box from the black box server to result in a second black box when the

first black box is not current.

153.   (Withdrawn) The method of claim 152 wherein the DRM system has

a previously installed black box prior to the requesting step, the method further comprising

determining prior to the requesting step that the previously installed black box is non-unique.

154.   (Withdrawn)   The method of claim 152 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is not current.

155.   (Original)   The method of claim 152 wherein the requesting step comprises requesting the black box by way of a network connection to the black box server.

156.   (Original)   The method of claim 155 wherein the requesting step comprises requesting the black box by way of an Internet connection to the black box server.

157.   (Withdrawn)   The method of claim 152 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the requesting step includes providing the public / private key pair of the first previously installed black box to the black box server, whereby the generated black box is provided with the public / private key pair of the first previously installed black box.

158.   (Withdrawn)   The method of claim 157 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the requesting step

Page 14 of 23

further includes providing the public / private key pair of the second previously installed

black box to the black box server, whereby the generated black box is also provided with the

public / private key pair of the second previously installed black box.

159.   (Withdrawn) The method of claim 152 wherein the received black

box includes an identifier indicative of currency.

160.   (Withdrawn) The method of claim 159 wherein the received black

box includes a version number.

161.   (Withdrawn) The method of claim 152 wherein the received black

box includes a digital certificate.

162.   (Withdrawn) The method of claim 161 wherein the received black

box includes a digital certificate proffering that such received black box should be trusted.

163.   (Withdrawn) The method of claim 152 wherein at least a portion of

the private key of the received black box is encrypted according to a code-based encryption

technique.

164.   (Withdrawn) The method of claim 163 at least a portion of the private

key of the received black box is encrypted according to software code associated with such

received black box, whereby adulteration of such software code prevents such private key

from being decrypted.

Page 15 of 23

165.   (Original)   The method of claim 152 wherein the received black

box is associated with the DRM system / computing device, whereby such received black box

is inoperable on another DRM system / computing device.

166.   (Original)   The method of claim 165 wherein the requesting step

includes providing information unique to the DRM system / computing device, and wherein

the received black box was generated based in part on the provided information, whereby the

received black box can recognize whether it is intended for the DRM system / computing

device upon which it is installed.

167.   (Original)   The method of claim 165 wherein the DRM system /

computing device is a first DRM system / computing device, wherein the received black box

is associated with the first DRM system / computing device and also with a second DRM

system / computing device, whereby the received black box is inoperable on another DRM

system / computing device which is not the first or second DRM system / computing device.

168.   (Currently Amended) A computer-readable medium having computer-

executable instructions thereon for performing a method in combination with a digital rights

management (DRM) system operating on a computing device, the DRM system requiring a

black box for performing decryption and encryption functions, the method for providing the

black box by a black box server and comprising:

receiving a request for [[the]] a first black box from the DRM system;

Page 16 of 23

generating the first black box, such generated first black box being unique and

having a public / private key pair and ~~functionality necessary to employ such~~ electronic code

for employing the key pair within the DRM system on the computing device; and

delivering the generated first black box to the DRM system, the delivered first

black box being installed by the DRM system in such DRM system,

the DRM system further providing code for periodically determining whether

the first black box is current or not current and for upgrading at least the public / private key

pair in the first black box from the black box server to result in a second black box when the

first black box is not current.

169.   (Original)   The method of claim 168 wherein the receiving step

comprises receiving the request by way of a network connection between the black box

server and the DRM system.

170.   (Original)   The method of claim 169 wherein the receiving step

comprises receiving the request by way of an Internet connection between the black box

server and the DRM system.

171.   (Withdrawn)   The method of claim 168 wherein the DRM system has

a first previously installed black box prior to the requesting step, the first previously installed

black box having a public / private key pair different from the public / private key pair of the

generated black box, and wherein the generating step includes providing the generated black

box with the public / private key pair of the first previously installed black box.

172.   (Withdrawn) The method of claim 171 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the generating step further includes providing the generated black box with the public / private key pair of the second previously installed black box.

173.   (Withdrawn) The method of claim 168 wherein the generating step includes providing the generated black box with an identifier indicative of currency.

174.   (Withdrawn) The method of claim 173 wherein the generating step includes providing the generated black box with a version number.

175.   (Withdrawn) The method of claim 168 wherein the generating step includes providing the generated black box with a digital certificate.

176.   (Withdrawn) The method of claim 175 wherein the generating step includes providing the generated black box with a digital certificate proffering that the generated black box should be trusted.

177.   (Withdrawn)   The method of claim 168 wherein the generating step

includes encrypting at least a portion of the private key of the generated black box according

to a code-based encryption technique.

178.   (Withdrawn)   The method of claim 177 wherein the generating step

includes encrypting at least a portion of the private key of the generated black box according

to software code associated with the generated black box, whereby adulteration of such

software code prevents such private key from being decrypted.

179.   (Original)   The method of claim 168 wherein the generating step

includes associating the generated black box with the DRM system / computing device,

whereby the generated black box is inoperable on another DRM system / computing device.

180.   (Original)   The method of claim 179 wherein the receiving step

includes receiving information unique to the DRM system / computing device, and wherein

the generating step includes generating the black box based in part on the received

information, whereby the generated black box can recognize whether it is intended for the

DRM system / computing device upon which it is installed.

181.   (Original)   The method of claim 179 wherein the DRM system /

computing device is a first DRM system / computing device, wherein the generating step

includes associating the generated black box with the first DRM system / computing device

and also with a second DRM system / computing device, whereby the generated black box is

DOCKET NO.: MSFT-0109/127334.9   PATENT
Application No.: 09/482,840
Supplemental Response

inoperable on another DRM system / computing device which is not the first or second DRM

system / computing device.